

★ All RrSG
content is proudly
human-generated

RrSG Explainer: Why Registrars Want to Mitigate DNS Abuse

I C A N N | R r S G

Registrar Stakeholder Group

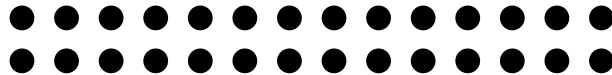
Why do registrars care?

- ★ DNS Abuse **hurts people.**
We want to Do The Right Thing
- ★ **We use the Internet too!**
We want a clean and safe Internet
- ★ DNS Abuse **costs us money**
- ★ DNS Abuse **harms our reputation**



There's a misconception that registrars profit off of DNS Abuse. Why?

Most online scams ultimately point to a domain name, so the registrar that sold the name is an easy target. But **the domain is just the visible part**: it's there in the phishing email, it shows up in the browser bar, and a lookup returns a registrar to write to. **Web hosting providers, payment processors, and others collecting the money sit further back in the chain and take much longer to identify—and they take longer to address DNS Abuse.** [Learn more.](#)

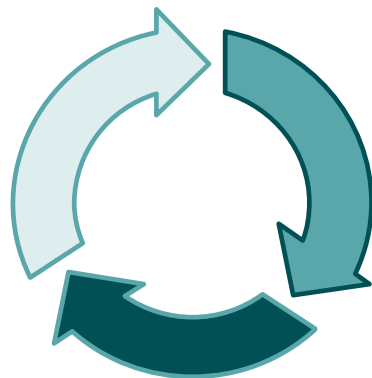


Registrar Motivations for maintaining a clean namespace

1. **Business continuity:** DNS Abuse causes the domain namespace to be untrustworthy and makes it harder to sell the legitimate services we offer (including domains, hosting, or email) as association with an untrusted provider harms our own customers.
2. **Reputation:** Blocklists are quick to add a provider to their blocklist—but slow to remove. We could lose customers because our services are blocked by up- or down-stream providers, even when the Abuse has been promptly mitigated.
3. **Payment provider access:** Payment providers can disallow payments due to association with threat actors, and high levels of questionable transactions may lead payment providers to charge higher rates or stop providing services to a registrar.
4. **Fraud:** A lot of DNS Abuse doesn't use legitimate payment methods—and it costs us money to get refunds for the use of falsified or stolen credit cards.
5. **Abuse attracts abuse:** Lack of mitigation efforts will attract more threat actors to the platform, increasing the rate of harm overall.
6. **Incentive for prompt attention:** Registries only offer refunds on domains caught and deleted in the first 5 days of their lifetime, and within limited volume thresholds.

Domain migrations: an ongoing challenge

- Malicious registrants do not settle. They concentrate on one registrar, but once that registrar identifies the pattern of their orders and closes the door, they just move to the next one and start again.
- If registrars welcomed their business, there would be no migration. Abusive domains would stay where they are, and be renewed year after year, at a registrar happy to have them.
- What the data shows instead is a small number of actors circulating through the market, looking for the least-defended entry point at any given moment, and being pushed out as each entry point is closed.



What the RrSG is doing to help fight DNS Abuse

Contract amendments

We proposed the [Framework](#) that led to the 2024 RAA DNS Abuse Amendments, and participated in their negotiation

1

Guidance & information

We built [ACIDTool](#) to help people identify where to report various types of Abuse, and we regularly post helpful info on [RrSG.org](#)

2

ICANN Groups

The RrSG and CPH maintain a DNS Abuse Subgroup, and contribute to ICANN PDP WGs, IRTs, and other sessions on this topic

3

Outside engagement

We engage with gTLD and ccTLD registries around the world, and participate in industry associations beyond ICANN

4

What we can all do to help fight DNS Abuse

Clear distinction between malicious and compromised domains

Suspending a compromised domain punishes a victim and takes down services that have nothing to do with the Abuse. These cases need notification and remediation, not the same treatment as a domain registered for malicious purposes. *Learn more:* [RrSG Explainer: Malicious vs Compromised Domains](#)

Well-evidenced Abuse reports

A report with the URL, timestamp, payload and the reason you believe the domain is malicious can be actioned in minutes. A report with just a domain name takes longer to investigate and often ends without action not because the registrar is unwilling but because they have nothing to act on. *Learn more:* [CPH Guide to Effective DNS Abuse Reports](#)

Work with the broader Internet Community

The domain is the cheapest and most replaceable component of an Abuse campaign. Web hosting, payment processors, and other monetisation are where the proceeds go, and where enforcement can change the economics for the bad actor rather than for the intermediary. *Learn more:* [Reporting Online Harm Flow Chart](#)